Ad Hoc Networks
Volume 163, 1 October 2024, 103606

A smart contract-based 6G-enabled authentication scheme for securing Internet of Nano Medical Things network

Neeraj Kumar, Rifaqat Ali

Show more

https://doi.org/10.1016/j.adhoc.2024.103606

Abstract

Nanotechnology has recently emerged as a pivotal field with wide-ranging implications. Its integration into the 6G-enabled Internet of Things (IoT) has given rise to the 6G-enabled IoNT (Internet of Nano Things) paradigm, impacting sectors such as healthcare, industries, smart homes, aerospace, and defense. This technology offers opportunities to revolutionize existing methodologies and enhance efficiency. Research efforts are now focusing on developing secure, scalable network infrastructures tailored for the healthcare sector at the nanoscale, leading to the concept of the Internet of Nano Medical Things (IoNMT). However, the unique characteristics of nanotechnology pose security challenges, particularly concerning privacy, confidentiality, dependability, latency, and the expensive consequences of blockchain-based storage. Authentication and transparency are vital for ensuring secure data handling in IoNMT networks, necessitating a secure access mechanism resistant to unauthorized interference. To tackle these challenges, this study proposes a smart contract-based authentication protocol

developed specifically for 6G-IoNMT networks. The framework aims to manage real-time information with minimal latency through decentralized peer-to-peer cloud servers while addressing security and privacy concerns. Thorough security and privacy assessments, including ROR model evaluations, Scyther tool analysis, and informal security evaluations, validate the protocol's effectiveness. Moreover, the simulation highlights that this protocol offers superior security and efficiency as well as energy consumption compared to existing protocols.

Introduction

The 6G-enabled Internet of Things (IoT) refers to a network comprising physical devices, vehicles, structures, and other elements equipped with sensors, software, and connectivity, enabling them to collect and exchange data [1]. This technology has transformed our lifestyles and work practices by introducing unprecedented levels of efficiency, automation, and convenience. Its impact spans across diverse sectors such as agriculture, industry, households, defense, and healthcare [2], [3]. As technology progressed, it gave rise to a new paradigm known as the Internet of Nano Things (IoNT) [4]. The IoNT involves integrating nanotechnology with the IoT, creating a network of interconnected nano-scale devices [5]. Essentially, the initial goal of IoNT is to collect and exchange data, similar to the internet of things devices. However, what distinguishes it is the scale, sensor capabilities, communication methods, and power usage, all contributing to a unique approach for data exchange. The nano-devices employed in IoNT are extremely small, functioning on a nano-dimension. This network comprises nanosensors responsible for basic computations and tasks, nano routers interconnected with other nano-devices, and a gateway serving as an aggregator. Data exchanged among these devices is transmitted from the gateway to servers such as edge or cloud servers for storage or further utilization [6].

IoNT finds applications across diverse fields, where its utilization in the healthcare sector is evident [6], [7]. In the healthcare sector, the emergence of the IoNT has led to the development of the Internet of Nano-Medical Things (IoNMT). IoNMT utilizes nano-devices and sensors capable of collecting and transmitting data at the molecular level. For example, nano-devices could be employed for more precise targeting of cancer cells or for early detection and monitoring of illnesses. In IoNT, two key communication techniques are nano-electromagnetic communication and molecular communication [8], [9]. Nano-electromagnetic communication utilizes electromagnetic waves, like radio

waves, at the nano-scale, posing challenges due to device size and power constraints. RFID and RedTacton are examples, with RedTacton offering faster data throughput and more stable connections [10], [11]. Terahertz (THz) communication, a newer technology, uses electromagnetic waves in the terahertz frequency spectrum, offering high penetration and data rates, useful for communication between nano-scale devices and gateways [12]. Molecular communication employs molecules as carriers of information, offering high concentration and localization. This is ideal for the IoNT, where devices are small, located in hard-to-reach places, and have very limited processing, storage, and battery capacities [13]. Combining both techniques enhances communication performance and network reliability. Nano electromagnetic communication ensures fast transmission over long distances, while molecular communication is energy-efficient for nano-devices, providing redundancy and uninterrupted communication in IoNT networks [14], [15].

Security is paramount in the IoNT due to the transmission of sensitive data, which could have devastating consequences if leaked or stolen. IoNT devices might be positioned where they can be accessed physically with minimal restrictions. Consequently, developers of cryptographic software for these devices should account for potential physical attack scenarios. Such attacks typically fall into two categories: active attacks, such as fault attacks, and passive attacks, which involve side-channel analysis (SCA), including power and timing analysis [16]. Additionally, ensuring the integrity of machine learning results is equally critical, as compromised outcomes could lead to significant issues. Recent research has shown that some machine learning algorithms can be compromised by augmenting their training datasets with malicious data, leading to a new class of attacks called poisoning attacks [17]. While some studies address security concerns, more research is needed [18]. Various concerns about security and privacy in molecular communication have been raised, prompting the development of secure protocols like the Diffie–Hellman algorithm [19]. Authentication is crucial but challenging in the IoNT due to difficulties in assigning unique identifiers to devices. One proposed solution involves assigning the same identifiers to devices at the equal distance from the router, simplifying authentication processes. Robust authentication mechanisms can prevent unauthorized access and data breaches, ensuring the overall security of IoNT networks and enabling further research in the field. Moreover, centralized storage in IoNMT raises significant security and privacy concerns, such as data confidentiality, breaches, and availability issues. Additionally, a single point of failure could severely disrupt the IoNMT network. Centralized systems require manual implementation of agreements and involve third-party systems to establish trust among

network entities. These issues can be mitigated with blockchain technology, which ensures data immutability through unalterable blocks [20], [21]. Smart contracts on the blockchain enforce agreements independently, while consensus protocols maintain data integrity. 6G-enabled IoT promises significant advancements in IoNMT development through ultra-high bandwidth, ultra-low latency, and high-density connectivity [22]. This enhances the security and reliability of patient health data, aiding doctors in informed decision-making. Blockchain technology offers swift information dissemination, robust security measures, resilience against single-point failures, disaster recovery capabilities, enhanced data traceability, cost-efficiency, and heightened data transparency within the realm of IoNMT.

Our study aims to implement a novel smart contract based authentication method at the nanoscale within the 6G-IoNMT network architecture as describe in Fig. 1. The architecture involves communication between nanoscale, microscale, and generic IoT devices (gateway node, cloud server), with distinct communication phases. We employ diffusion-based molecular communication for nano-devices to resist remote or proximity attacks, while other devices use electromagnetic communication. Our goal is to integrate authentication throughout the communication process, though concrete results on cryptographic operation times are lacking. We aim to enhance authentication methods for nanoscale devices by integrating blockchain technology with existing cryptographic algorithms. Given the limited power and storage capabilities of devices in the IoNMT network, our authentication scheme prioritizes lightweight cryptographic protocols for efficiency and effectiveness [23]. Currently, the framework employs ECC for secure key exchange, acknowledging the need to transition to post-quantum cryptography (PQC) for long-term security [24], [25]. ECC stands out as a promising choice for standardized PQC applications due to its ability to maintain key advantages of traditional ECC, such as small key and signature sizes, promoting efficient computation and communication [26], [27]. Furthermore, ECC offers forward secrecy, ensuring the security of session keys even if long-term keys are compromised in the future. These attributes make ECC well-suited for applications demanding robust security with minimal resource consumption, such as the Internet of Nano Medical Things (IoNMT).

However, as quantum computing progresses, PQC will become indispensable to counter quantum threats [28], [29]. Although typically more resource-intensive, PQC algorithms are designed to withstand quantum attacks and will be crucial for maintaining cryptographic system security in the future. Introducing security functionalities inevitably adds computational and communication overheads, impacting network

performance. Our study includes an initial assessment of these implications within a representative IoNMT scenario, aligning with prior research on communication and cryptographic operations at the nanoscale [8], [9]. Additionally, the paper's main contributions are detailed in the subsequent subsection.

Over the years, various authentication and key agreement techniques have emerged in the context of 6G-enabled IoT [30], [31]. The rise of this new technology has transformed the IoT industry, shifting focus towards IoNT following significant growth in IoT. Yet, new technology introduces both opportunities and challenges [10]. Additionally, as stated in [8], a secure architecture has been proposed as a foundation for advancing this innovative technology, along with an authentication and key agreement scheme. Considering this, we observed several gaps, including a significant research gap in the IoNMT network, where no blockchain-based authentication scheme has been introduced to our knowledge. The following outlines some of the notable contributions of the research:

- We introduce a novel secure and lightweight blockchain-based authentication and key agreement scheme for 6G-IoNMT networks (IoNMT-BAS), tailored to the capabilities of nano-scale devices. This scheme comprises three phases. The initial phase involves authentication between the nano device and nano router. The next phase is dedicated to key agreement between the nano router and gateway node, while the third phase entails blockchain formation by the cloud server using information obtained from the gateway nodes.

- In proposed blockchain-based model for IoNMT networks, we integrate a phase enabling the dynamic inclusion of nano devices and nano routers. During this stage, should a nano router detect any questionable activity from a nano device, or vice versa, it has the capability to swiftly notify the blockchain network to commence revocation protocols.

- We conduct a thorough assessment of our protocol's security, utilizing informal and formal evaluations. In proposed protocol's formal security analysis, we leverage the Real or Random Oracle model (ROR) in conjunction using the Scyther simulation tool. Collectively, these evaluations confirm the protocol's robustness against various active and passive attacks.

- We use the Multi-Precision Integer and Rational Arithmetic Cryptographic Library (MIRACL) to simulate our proposed protocol. Through a detailed comparative analysis of factors like “security and functionality attributes”, “communication costs”, “computational costs”, and energy consumption between IoNMT-BAS and other relevant approaches, proposed research highlights the superiority of IoNMT-BAS over existing protocols.

The rest of this paper is organized as follows: Section 2 provides a thorough review of relevant literature. In Section 3, we outline the system model, covering the nano-device architecture, network model, communication model, and security aspects. Section 4 introduces a new blockchain-based authentication framework for IoNMT networks. In Section 5, we provide both formal and informal examinations of security. While Section 6 presents performance assessments, comparisons, and outcomes from experimental simulations. Ultimately, our work is concluded in Section 7.

Section snippets

Literature survey

The emerging evolution driven by nanotechnology is still in its early stages in terms of establishing suitable network architectures, protocols, and effective security and privacy capabilities. Additionally, achieving interconnection and interoperability between nano-devices and existing communication networks and paradigms necessitates the design and development of new IoNT architectures, protocols, and standards. An initial proposal is outlined in [4], where the authors identify the main …

System model

This segment comprises four distinct parts: firstly, the architecture of the nano-device, illustrating the constituent elements employed in such devices; secondly, the network model, delineating the design of the IoNT environment; thirdly, the communication model, explicating the interaction among devices within the Internet of Nano Things setting; and finally, security model, encompassing the security prerequisites sought through our proposed authentication protocol. …

The proposed scheme

This section provides a thorough discussion of the suggested “A Smart Contract-based 6G-enabled Authentication scheme for IoNMT Network” is presented. The definitions of symbols used throughout the article are detailed in Table 1. Moreover, a thorough schematic depiction of the suggested framework is shown in Fig. 6. …

Security analysis

This section will provide formal as well as informal security analyses, as detailed below: …

Performance evaluation

This section features a comparative analysis of the communication and computational costs associated with the following two scenarios:

- **Scenario 1:** Authentication between $\boldsymbol{ND}$ and $\boldsymbol{NR_i}$. …
- **Scenario 2:** Key agreement between $\boldsymbol{NR_i}$ and $\boldsymbol{GWN_j}$. …

…

Conclusion

The integration of nanodevices into IoNMT brings forth various security and privacy challenges, including constraints on lightweight design, transparency issues, unauthorized data access, and message tampering. Recent literature delves into various authentication and key agreement schemes tailored for IoT environments, with only a handful specifically designed for IoNMT networks. However, not all of these schemes cover all the mentioned features, and some do not incorporate blockchain …

Ethical approval

This section is not applicable as the study did not involve any human or animal subjects. …

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. …

CRediT authorship contribution statement

Neeraj Kumar: Writing – original draft, Visualization, Validation, Software, Methodology, Formal analysis, Conceptualization. **Rifaqat Ali:** Visualization, Supervision, Project administration, Investigation. …

Declaration of competing interest

There is no Conflict of Interest. …

Acknowledgments

We are grateful to the University Grants Commission (UGC), India for providing the first author with a fellowship. …

Mr. Neeraj Kumar did M.Sc. (Master of Science) from Motilal Nehru National Institute of Technology Allahabad, Uttar Pradesh, India. Currently, he is pursuing Ph.D. from the department of Mathematics and Scientific Computing, National Institute of Technology Hamirpur, Himachal Pradesh, India. His research area is Cryptography and Blockchain Technology. …

…

…

Recommended articles

References (58)

KumarN. *et al.*
Blockchain-enabled authentication framework for maritime transportation

system empowered by 6G-IoT
Comput. Netw. (2024)

GalalA. *et al.*
Nano-networks communication architecture: Modeling and functions
Nano Commun. Netw. (2018)

DresslerF. *et al.*
Connecting in-body nano communication with body area networks: Challenges and opportunities of the internet of nano things
Nano Commun. Netw. (2015)

SicariS. *et al.*
Beyond the smart things: Towards the definition and the performance assessment of a secure architecture for the internet of nano-things
Comput. Netw. (2019)

KumarV. *et al.*
IoV-6G+: A secure blockchain-based data collection and sharing framework for internet of vehicles in 6G-assisted environment
Veh. Commun. (2024)

AliR. *et al.*
A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring
Future Gener. Comput. Syst. (2018)

JornetJ.M. *et al.*
Phlame: A physical layer aware mac protocol for electromagnetic nanonetworks in the terahertz band
Nano Commun. Netw. (2012)

CaoS. *et al.*
Cloud-assisted secure ehealth systems for tamper-proofing EHR via blockchain
Inform. Sci. (2019)

ChenZ. *et al.*
A blockchain-based preserving and sharing system for medical data privacy
Future Gener. Comput. Syst. (2021)

ServatiM.R. *et al.*
ECCbAS: An ECC based authentication scheme for healthcare IoT systems
Pervasive Mob. Comput. (2023)

View more references

Cited by (2)

BBAD: Blockchain-based data assured deletion and access control system for IoT ↗
2025, Peer-to-Peer Networking and Applications

A Review of 6G and AI Convergence: Enhancing Communication Networks With Artificial Intelligence ↗
2025, IEEE Open Journal of the Communications Society

Mr. Neeraj Kumar did M.Sc. (Master of Science) from Motilal Nehru National Institute of Technology Allahabad, Uttar Pradesh, India. Currently, he is pursuing Ph.D. from the department of Mathematics and Scientific Computing, National Institute of Technology Hamirpur, Himachal Pradesh, India. His research area is Cryptography and Blockchain Technology.

Dr. Rifaqat Ali is presently working as an Assistant Professor in the Department of Mathematics and Scientific Computing, National Institute of Technology, Hamirpur, Himachal Pradesh, India. He did his Ph.D. from the Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines), Dhanbad in 2018. He has more than 5 years of teaching and research experiences, and contributed a several research papers in many reputed journals and international conference proceedings. His main research interest includes Cryptography and Network security.